Failure to Warn You Might get Pwned: Vulnerability Disclosure and Products Liability in Software

@wendyck
wendy@wendyk.org
3L, George Mason University School of Law

This is not legal advice

I am not (yet) a lawyer, this is not legal advice.

But I am interested in your thoughts on this topic- please tweet me or find me around this weekend.

@wendyck

https://twitter.com/WeldPond/status/650638805528125440

Vulnerability Disclosure

Software has vulnerabilities; these are sometimes found and sometimes patched.

This talk is not about the CFAA, it's about consumer protection & tort law.

Can consumers who bought defective software recover damages?

Right now, it’s very hard (or impossible) to recover for defective software outside of a sales or other contract with the seller. This talk will explain why, and look at what might change.

Buckle up, this is a whole law school course at high speed.

Torts: redress of physical suffering

Did someone or something physically harm you?
If yes: proceed to go.
If not, there's a tort doctrine that may cause you problems….

Pure Economic Loss

one of the biggest reasons why we don’t have product liability for software: no physical harm or no contract = hard to get recovery

There is also: Contract law

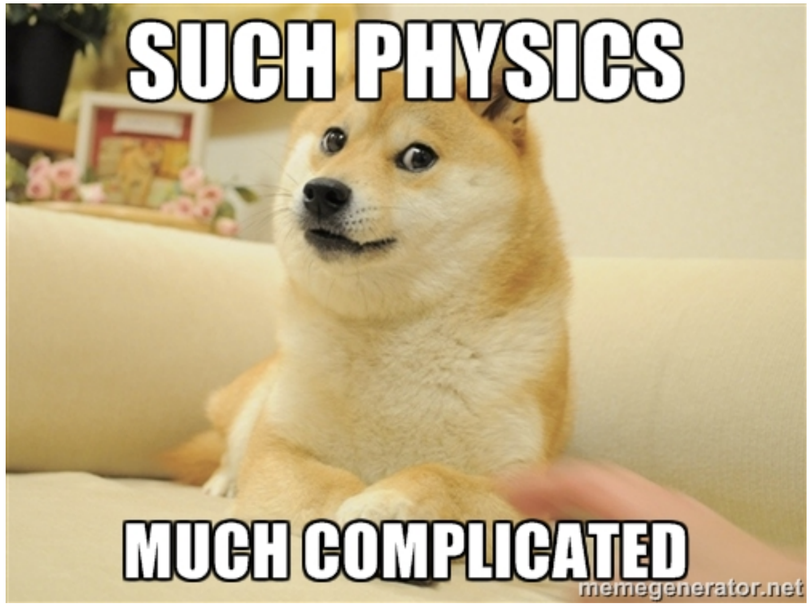
EULAs, clickwrap, etc shield software makers from a lot of liability.

If you have a service agreement or a business relationship, you might be able to recover under that.

Not as consumer-friendly as product liability tort law, though.

So we have two restrictions:

- Contract law
- Physical harm



Products Liability Law:

How consumers of defective products use the legal system.

The general idea: if your lawn mower hurts you, you can sue the manufacturer to recover. Or the store that sold you the lawn mower.

Tries to be consumer friendly.

Consumers allege one of three types of harm:

1. Manufacturing defects
2. Design defects

3. Failure to Warn: Business failed to let consumers know that a widget might hurt them if used in a particular way

Why can’t I sue a software company if the tool they wrote crashes all the time?

Products liability is focused on physical harms

And, until recently, software was unlikely to physically harm you

IOT may change that, and products liability might someday be found to apply to software

Contract Law & Product Liability

There was a shift in the early 1900s to remove some contract law restrictions from product liability suits as society and manufacturing changed.

Product Liability law serves an insurance function; want incentives make products safer

So...

How does this relate to vulnerability disclosure?

Stories abound of software vendors ignoring these vulnerability reports for months or years, leaving consumers at risk of independent exploitation until patches are developed & released.

Consumers have had little voice in this standoff.

Under a Failure to Warn claim, could consumers argue that vendors should have alerted them of risks, and how to mitigate?

Failure to warn variants

1. Risk reduction warning

   “if you use our chainsaw, wear goggles, wear hand protection, don’t stand on a ladder”

2. Informed choice warning

   “this product is dangerous in this way. can’t reduce risk, but you should know” (i.e. pharmaceutical warnings)

Vuln disclosure risk reduction warning

“if you use our WonderWidgetSoftware, turn off features x & y and don’t run it with Java v N”

Vuln Disclosure Informed choice warning

“WonderWidgetSoftware has a vulnerability in that attackers can spoof a wifi hotspot and get your wifi credentials. You can’t tweak any settings to prevent this behavior, but you should know.”

What would these warnings look like?

Liability keyed off the idea that company knew or should have known that it should have given better warnings

But, different users need different kinds of instructions or warnings:
A big problem is some products are used both by experts & by lay people

Products Liability is generally Strict Liability

If you’re not a lawyer, what does that mean?

Strict Liability:

liability without fault

Why Strict Liability?

instead of negligence (liability based on defendant's bad behavior)

- **makes bad products pricier (depends on assumption that consumers underestimate risk) (also considering that people have same risk utility curves)**
- **reduce transactions costs (easier to prove SL than negligence)**
- **insurance function: loss spreading**
- **fairness: not fair someone is injured by product & not compensated**
- **reasonable consumer expectations for safety**

Strict vs Balancing

- But Products Liability is often not really “strict” (see: you can still buy knives, other “dangerous” products, if they have social utility. Dangerous-low-utility products leave market. ie lawn darts)

Liability is keyed on foreseeable use

Broken coke bottle case:

"manufacturer incurs an absolute liability when an article that he has placed on the market, knowing that it is to be used without inspection, proves to have a defect that causes injury”

If you use the product in a completely ridiculous way, and are injured, strict liability is not so strict.

Tradeoffs

Failure to warn doctrine takes into consideration cost-benefit analysis that might be adapted to vulnerability disclosure.

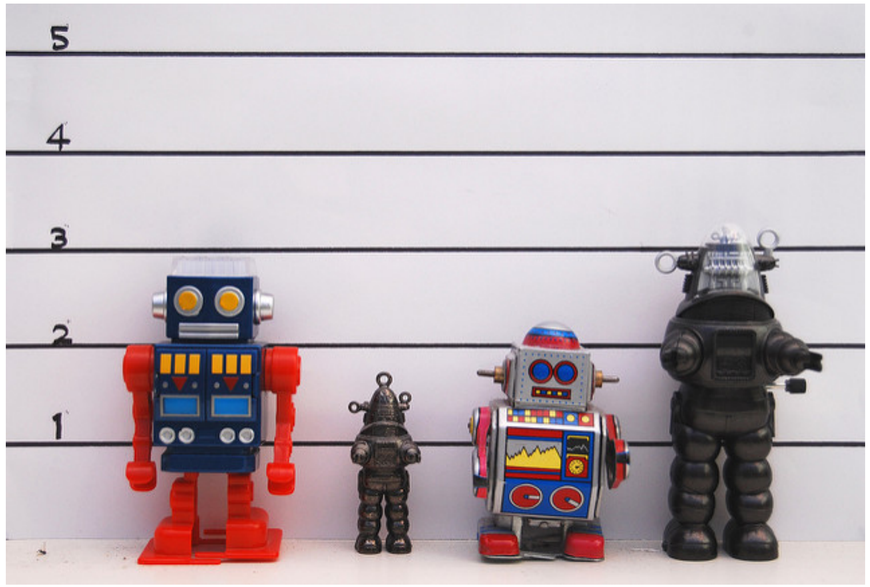
Obvious & generally known risks: What's a sufficient warning?

Can a lay jury decide what an adequate warning is for a technical issue?

Bsides Charm- @wendyck

How would this even work?

Researcher reports a vuln
Company decides it’s a Won’t Fix for some reason
Company issues no warnings
User is pwned
???
Liability?



How would this even work?

http://artfulhacker.com/post/142519805054/beware-even-things-on-amazon-come

PROBLEMS

How do we protect consumers without overwhelming them?

What about mean-time-to-exploit?

Does every company need a security contact form?

What about open source?

What about coordinated disclosure?

Policy reasons: fear of stifling innovation

Companies have been concerned about imposing any kind of liability - fear of stagnation due to designing overly-safe software in response to the imposition of tort liability

Will IOT Cause a shift?

- Mass production and supply chains revolutionized products liability in the last century
- Will cases of physical harm develop a framework under which non-physical harm cases will arise?
  Or will the harm requirement stay?
- Do we want to use Failure to Warn or is another doctrine a better framework?

If you'd like to know more

I also wrote an article this summer that expands on some of this:

[Why can't you sue software makers for bugs? And how the law might evolve in the IoT era]

NTIA's Vulnerability Disclosure Multistakeholder Groups

https://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-cybersecurity-vulnerabilities

Thank you & questions

@wendyck

wendy@wendyk.org